CENTRAL BANK DIGITAL CURRENCIES: THE THREAT FROM MONEY LAUNDERERS AND HOW TO STOP THEM

By Yaya J. Fanusie[*]

November 2020

If or when a central bank digital currency is deployed in a major economy such as the United States, there will be unintended consequences. Financial regulators should anticipate these threats and employ policy responses attuned to digital innovation in order to mitigate inevitable illicit behavior.

Digital currency appears to be the future of money. Efforts to merge monetary policy and instruments with computer-science-driven financial technology are gaining momentum globally.[1] Central banks in large and small economies alike are proposing to revamp their monetary systems by deploying new types of digital tokens that would be managed by a single authority and designed for wide-scale retail use. Unlike independent cryptocurrencies such as Bitcoin, central bank digital currency (CBDC) has a high chance of national adoption precisely because it would be issued by a nation's monetary authority, with its value backed by government fiat and its use encouraged by public policy.

Any large economy that builds and deploys a CBDC is likely to encounter new financial crime risks. Compared to physical cash, CBDCs will in certain respects make it easier for regulators to fight money laundering, and key technical aspects of CBDCs will hinder some traditional illicit financial techniques. But CBDCs will nevertheless be a tempting target for bad actors, both state and non-state, who will adapt their methods accordingly. In particular, the unique technical features that

[*] Adjunct Senior Fellow, Center for a New American Security.

[1] *CBDC Tracker - Central Bank Digital Currencies*, http://cbdctracker.org.

CBDCs will add to fiat money—such as wallet programmability and microtransactions (the ability to transact at volumes below a penny)—will enable more intricate money laundering schemes.

But these money laundering risks should not dissuade governments from developing CBDCs, which could provide substantial benefits to consumers and businesses. Anti-money laundering (AML) professionals can fine-tune transaction monitoring to account for CBDC capabilities. And by understanding this new evolutionary phase of money, policymakers can set appropriate compliance standards to cultivate high integrity for the financial technology industry that will likely expand around CBDC applications. By anticipating new layers of financial crime, financial regulators can, in cooperation with the private sector, employ policy responses attuned to digital innovation and mitigate the inevitable illicit behavior that will touch CBDC platforms.

WHAT IS A CBDC, AND WHY NOW?

The financial system is already replete with digital payments. What distinguishes CDBCs from current digital transactions involving government-backed fiat currency is the possibility of *tokenization:* "the act of turning an asset, good, right, or currency into a representation with properties that suffice to attest to and transfer ownership."[2] A CBDC dollar could be tokenized to represent a U.S. Federal Reserve–backed dollar; the CBDC dollar would thus be immediately acceptable and redeemable for its stated value by financial institutions and merchants, just as when they accept physical cash. A token-based system gives the public direct digital access to central bank reserves just as in using cash banknotes.[3]

This is not how the majority of digital financial transactions work today. Instead of being token based, today's digital payment infrastructure is largely account based. Bank wire transfers, debit and credit card payments, and PayPal transactions are in fact *obligations* of one party to pay another. Merchants, banks, and payment processing companies accept these digital payment methods at the point of sale, but there is a separate process that settles these obligations, balancing the accounts represented in the transactions. This is part of the reason why electronic fund transfers often take multiple days to deposit into bank accounts and why debit card payments made on a weekend will show up as "processing" in the card owner's account until the individual's bank opens on a Monday.

---

[2] Charles H. Giancarlo et al., "Exploring a US CBDC," Digital Dollar Foundation, May 2020, static1.squarespace.com/static/5e16627eb901b656f2c174ca/t/5f0c5d052d6235002637d0f6/1594645769165/Digital-Dollar-Project-Whitepaper_vF_7_13_20.pdf.

[3] Giancarlo et al., "Exploring a US CBDC."

This process of crediting, debiting, and settling the accounts involving digital payments is also the source of the fees that payment processors charge.

Tokenizing digital currency is accomplished using some of the same technology that underpins Bitcoin. The Bitcoin software protocol, designed in 2008, eliminated the need for a centralized entity to authenticate and settle digital transactions between two parties. The protocol enables parties to transfer ownership of Bitcoin tokens directly to others, with all transactions authenticated and recorded in an online decentralized ledger, commonly referred to as a blockchain.[4] Like Bitcoin, CBDCs would use public key cryptography to validate access to the digital currency.

But CBDCs would operate differently from Bitcoin in several important respects. First, Bitcoin and most other cryptocurrencies are independent protocols, not owned by any one entity and usually run by an informal association of software developers that anyone can join if they have the requisite technical knowledge of the protocol. CBDC systems would be developed and controlled by central banks. Second, Bitcoin transactions are pseudonymous, with no real identities attached to the blockchain. CBDCs would associate real identities with transactions so as to conform to AML regulations and facilitate permissioned access to the financial system. Third, Bitcoin uses proof-of-work "mining" to enable decentralized ledger authentication. This would not be required for CBDCs.

In short, as one central bank put it, a CBDC would be "a banknote, but in digital form."[5] By picking and choosing from aspects of cryptocurrency technology, CBDC proponents are developing a new form of money that financial authorities would continue to manage.

According to ConsenSys, a U.S.-based blockchain software development firm, CBDCs offer several benefits for central banks. These include reducing settlement risk in interbank payments, enabling direct distribution of reserve money to individuals, reducing costs in cross-border remittances, and encouraging more competition and innovation in the broader financial sector. Additionally, countries with weak economies are seeing private-sector-issued digital tokens (like Bitcoin) gaining traction as alternative payments or value storage, leading to waning monetary stewardship and

[4] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," bitcoin.org/bitcoin.pdf.
[5] Danny Nelson, "Canada's Central Bank Is Serious About Designing a CBDC, Job Posting Reveals," CoinDesk, June 16, 2020, www.coindesk.com/bank-of-canada-central-bank-digital-currency-project-manager.

regulatory effectiveness. For such countries, building a CBDC would encourage more of the public to operate within the nation's financial system instead of through independently run cryptoassets.[6]

Long-standing trends and recent economic developments are driving the rise of CDBCs. One trend is the steady rise[7] of noncash payments in commerce. Consumer preferences are driving much of this cash decline. Not only is paying by card instead of cash usually quicker, but more people are also purchasing goods and services online, where cash payments are not possible. This trend is accelerating with the coronavirus pandemic.[8]

Another influence is financial regulators' aim to limit money laundering through cash. From the perspective of strategies to counter money laundering and terrorist financing, cash is a risky form of payment. There have been several efforts to pull large-denomination bills from circulation. India banned the use of 1,000 and 500 rupee notes in 2016.[9] The European Union started phasing out the issuance of 500 euro notes that same year.[10] And while criminals and terrorists also use bank wire transfers, credit cards, checks, and other payment methods, users typically must register an identity with a third party to access them, providing a paper trail that is less likely with cash transactions. The anonymity of physical cash makes it an attractive money laundering instrument.

Policymakers also are prioritizing payment efficiency in providing economic relief. When the United States passed legislation in early 2020 to provide economic relief in response to coronavirus pandemic, some legislators suggested that the government should set up accounts at the Federal Reserve for payment recipients.[11] This idea did not make it into the final legislation, and members of Congress continued to grapple with the best ways to disburse relief payments into the summer of

---

[6] Matthieu Bouchaud et al., "Central Banks and the Future of Digital Money," ConsenSys, January 2020, pages.consensys.net/central-banks-and-the-future-of-digital-money.
[7] David W. Perkins, *Long Live Cash: The Potential Decline of Cash Usage and Related Implications*, Congressional Research Service, May 10, 2019, fas.org/sgp/crs/misc/R45716.pdf.
[8] Liz Alderman, "Our Cash-Free Future Is Getting Closer," *New York Times*, July 6, 2020, www.nytimes.com/2020/07/06/business/cashless-transactions.html.
[9] Justin Rowlatt, "Why India Wiped Out 86% of Its Cash Overnight," BBC News, Nov. 14, 2016, www.bbc.com/news/world-asia-india-37974423.
[10] Chris Cottrell and Hardy Graupner, "ECB Phases Out 500-Euro Banknotes," Deutsche Welle, April 5, 2016, www.dw.com/en/ecb-phases-out-500-euro-banknotes/a-19233831.
[11] Mike Orcutt, "We Just Glimpsed How a 'Digital Dollar' Might Work, Thanks to Coronavirus," *MIT Technology Review*, April 9, 2020, www.technologyreview.com/2020/03/26/950277/we-just-glimpsed-how-a-digital-dollar-might-work-thanks-to-coronavirus/.

2020.[12] The U.S. Senate Banking, Housing, and Urban Affairs Committee held a hearing in June 2020 on "The Digitization of Money and Payments" where expert witnesses discussed benefits and challenges of the march toward more digital payment systems, including a possible digital dollar.[13] Some of the witnesses argued that more digitization of payment systems would give better financial access to poorer individuals and communities.[14]

Rising central bank interest in the potential of CBDCs is widespread.[15] The Bank for International Settlements in January 2020 published a survey of advanced economy and emerging market central banks. It found that 80 percent of central banks in 2019 were researching CBDCs, compared to 70 percent a year earlier.[16] The bank's annual economic report for 2020 stated that "CBDCs can foster competition among private sector intermediaries, set high standards for safety and risk management, and serve as a basis for sound innovation in payments."[17] The bank also announced in mid-2020 that it was expanding its locations for international Innovation Hubs, which aim to spur collaboration between central banks on technological research into developments such as digital currencies.[18]

Information about possible CBDC architecture is now plentiful. Major central banks as well as financial technology industry groups have published papers suggesting CBDC technical and policy frameworks. For example, the Bank of England—the United Kingdom's central bank—released a discussion paper describing a potential digital currency version of the British pound.[19] The Digital

---

[12] "The Digitization of Money and Payments": Hearing Before the Committee on Banking, Housing, and Urban Affairs, 116th Congress, June 30, 2020, www.banking.senate.gov/hearings/the-digitization-of-money-and-payments.
[13] "The Digitization of Money and Payments."
[14] Nikhilesh De, "Witnesses Will Vouch for Stablecoins, Digital Dollars in US Senate Hearing Tuesday," CoinDesk, June 30, 2020, www.coindesk.com/witnesses-will-vouch-for-stablecoins-digital-dollars-in-us-senate-hearing-tuesday.
[15] Sarah Allen et al., "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations" (Global Economy & Development Working Paper 140), Brookings, July 2020, www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC_Final-for-web.pdf.
[16] Codruta Boar et al., "Impending Arrival – a Sequel to the Survey on Central Bank Digital Currency" (BIS Papers No. 107), Bank for International Settlements, January 2020, www.bis.org/publ/bppdf/bispap107.pdf.
[17] Bank for International Settlements, "Central Banks and Payments in the Digital Era," *BIS Annual Economic Report 2020*, www.bis.org/publ/arpdf/ar2020e3.pdf.
[18] Bank for International Settlements, "BIS Innovation Hub to Expand to New Locations in Europe and North America" (press release), June 30, 2020, www.bis.org/press/p200630a.htm.
[19] Bank of England, "Central Bank Digital Currency Opportunities, Challenges and Design," March 2020, www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf.

Dollar Project, a nonprofit association made up of financial industry leaders and former U.S. financial regulators, produced its own white paper suggesting an overall framework for a digitized U.S. dollar.[20] The European Central Bank is also studying the digitization of fiat currency[21] and has published a proof-of-concept paper about how privacy could be preserved in a CBDC system for the euro.[22] Various think tanks[23] and cryptoasset industry publications[24] have also published in-depth reports on CBDC developments. These papers, as well as writings by the International Monetary Fund,[25] give clear insight into how central bankers, economists, and financial technologists are conceptualizing CBDC frameworks and designs.

Many CBDC pilots are already occurring. The People's Bank of China has been testing its digital currency in selected cities since early 2020.[26] Canada in mid-2020 posted vacancies for a manager[27] and for technical staff[28] for a planned effort to develop a CBDC. In 2019 the Bank of Canada had partnered with the Monetary Authority of Singapore on a proof of concept to test out cross-border transfers of CBDC payments between central banks.[29] In recent months, central banks in smaller

[20] Giancarlo et al., "Exploring a US CBDC."
[21] Yves Mersch, "An ECB Digital Currency – a Flight of Fancy?" (speech), European Central Bank, May 11, 2020, www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511~01209cb324.en.html.
[22] European Central Bank, 2019, *Exploring Anonymity in Central Bank Digital Currencies*. https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf.
[23] Allen et al., "Design Choices for Central Bank Digital Currency."
[24] Ryan Todd and Mike Rogers, "A Global Look at Central Bank Digital Currencies," The Block Research, August 2020, www.tbstat.com/wp/uploads/2020/08/The-Block-Research-CBDC-Report-From-Iteration-to-Implementation_v1.04.pdf.
[25] John Kiff et al., "A Survey of Research on Retail Central Bank Digital Currency," International Monetary Fund, June 26, 2020, www.imf.org/en/Publications/WP/Issues/2020/06/26/A-Survey-of-Research-on-Retail-Central-Bank-Digital-Currency-49517.
[26] Jonathan Cheng, "China Rolls Out Pilot Test of Digital Currency," *Wall Street Journal*, April 20, 2020, www.wsj.com/articles/china-rolls-out-pilot-test-of-digital-currency-11587385339.
[27] Nelson, "Canada's Central Bank Is Serious About Designing a CBDC."
[28] "Research and Development Technologist, CBDC Job in Edmonton, AB at Bank of Canada," ZipRecruiter, 2020, www.ziprecruiter.com/c/Bank-of-Canada/Job/Research-and-Development-Technologist,-CBDC/-in-Edmonton,AB?jid=1daf79c88ae4ce7d.
[29] Scott Hendry and Sopnendu Mohanty, "Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies," Accenture, 2019, www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf.

economies as diverse as the Bahamas,[30] Kazakhstan,[31] Lithuania,[32] the Philippines,[33] and Sri Lanka[34] have announced formal steps to explore or pilot digital currencies.

HOW WILL CBCDS WORK?

The specific technical architecture and management policies for CBDCs are still being researched by individual nations and could end up taking various forms. There is, however, enough information in recent central bank statements and CBDC discussion papers to posit a general technical model and policy framework to inform illicit finance threat projections. This paper envisions a CDBC with the following features:[35]

- **The CBDC will be for retail use.** While some CBDC experiments focus on wholesale use (just between banks), the CBDC focused on here will be for retail transactions. Everyday individuals and nonbank businesses will hold and use the CBDC.

---

[30] Central Bank of The Bahamas, 2020, www.centralbankbahamas.com/news?id=16660.
[31] Ting Peng, "Kazakh Gov Plans to Double Its Investment in Digital Currency Mining," Cointelegraph, July 1, 2020, cointelegraph.com/news/kazakh-gov-plans-to-double-its-investment-in-digital-currency-mining.
[32] Andrius Sytas, "Lithuania Dabbles in Crypto-Coin as Central Banks Look for Ways to Fend off Facebook," Thomson Reuters, July 2, 2020, www.reuters.com/article/us-eu-cryptocurrency-lithuania/lithuania-dabbles-in-crypto-coin-as-central-banks-look-for-ways-to-fend-off-facebook-idUSKBN2431RF.
[33] Siegfrid Alegado, "Philippines Central Bank Mulls Issuing Its Own Digital Currency," Bloomberg, July 29, 2020, www.bloomberg.com/news/articles/2020-07-29/philippines-central-bank-mulls-issuing-its-own-digital-currency.
[34] Nishel Fernando, "Monetary Board to Consider 3 Shortlisted Tech Firms to Develop PoC of Blockchain-Based Shared KYC Facility," *Daily Mirror*, July 2, 2020, www.dailymirror.lk/business-news/Monetary-Board-to-consider-3-shortlisted-tech-firms-to-develop-PoC-of-blockchain-based-shared-KYC-fa/273-191054.
[35] A key assumption is that the CBDC will be launched in a liberal democracy with a free-market system. Although China's planned digital currency is closer to implementation than is the CBDC of any other major advanced economy, there is scant official public information about how it will work. China's central bank has not released a formal document explaining the features of its digital currency electronic payment (DCEP) system. Still, the features of the digital renminbi highlighted in statements by Chinese government officials and in Chinese press reporting mirror much of the same structure proposed in discussions about digitizing the dollar, pound, or euro. However, the illicit financing scenarios discussed in this paper are likely to be most relevant to societies where both constitutional power and societal expectations constrain government authority and limit law enforcement activity vis-à-vis civil liberties.

- **The CBDC distribution will have two tiers.** In the first tier, the central bank will create the digital tokens and provide them to payment interface providers, which will be regulated private-sector firms such as financial institutions, money service businesses, payment processors, and digital wallet companies. The central bank will provide a software interface for these firms to directly acquire CBDC. In the second tier, the payment interface providers will give the public access to CBDC. Payment interface providers will provide the platforms—most likely software-based wallets—through which individuals and entities transact in CBDC.

- **Payment interface providers will enforce AML controls.** Payment interface providers will comply with AML rules and sanctions requirements. Customers will go through a "know-your-customer" process so that the payment interface provider will have personal identification information for its individual users. CBDC software will prevent transactions with wallets that have been designated under the sanctions program of the central bank's nation.

- **Technology and law will protect user privacy from government surveillance.** The CBDC technology will not give the central bank real-time or direct access to the identities of CBDC users. The government will need to follow a formal legal process by way of subpoena power to acquire personal and transactional information, similar to current restrictions around government acquisition of bank account information.

- **The CBDC ledger data will not be public.** Whether the CBDC uses a centralized or distributed ledger on its back end, the transaction data will not be publicly viewable. As with today's payments system, individual financial institutions and money service businesses will have access to the transaction histories of only their customers and will have to protect them just as they do currently. Parties will not be able to see the balances and transaction histories of their counterparties.

- **The CBDC will be token based.** Although account-based CBDCs are being explored,[36] the CBDC model discussed in this paper is for a tokenized digital asset, recognized as legal tender in the jurisdiction. The CBDC will use cryptographic signatures to allow for tokenization and to prevent duplication of the asset. If a distributed ledger is involved in the CBDC, any direct access to the ledger will be permissioned, that is, restricted to parties chosen by the central bank.

[36] Tony McLaughlin, "Two Paths to Tomorrow's Money," *Citi*, forthcoming journal article.

- **The CBDC will incorporate programmable money.** The CBDC will have some element of smart-contract programmability, allowing for payment interface providers to build a variety of software services for CBDC users. Software developers will be able to write simple if-then programs into transaction arrangements and build these into customers' wallets. New business models and services will result from the ability to program bespoke payment arrangements and to create wallet applications that specialize in certain types of payments.

- **The CBDC will enable micropayments.** The CBDC will be able to divide into extremely small portions. For example, a CBDC dollar could be broken down into .00000001 cents to transact with an "internet of things" application that might require a stream of regular but tiny payments.

- **There will be no purely anonymous wallets.** The CBDC will be held and transmitted in digital wallets that are built and managed by payment interface providers. Every wallet engaged in transactions will have personal identification data attached to it, held by the payment interface provider and shared only in accordance with AML and privacy requirements. It will not be possible for someone to hold CBDC outside of a platform requiring know-your-customer data on its users.

- **Unhosted wallets will be possible.** In most cases, CBDCs will be "hosted," that is, held in wallets with private keys managed by the payment interface provider. However, there will be an option for noncustodial, unhosted wallets in which users control their own private keys. Unhosted wallets may be riskier because users could lose access to the tokens if they lose their private keys. But this option may be attractive for users seeking stronger security of their assets against cyber hacks and, as recipients of CBDC, looking to imitate the transactional irrevocability that physical cash exhibits. Such software will still be offered by a payment interface provider, which will gather know-your-customer information on the user before providing the wallet. An array of regulatory restrictions may be programmed into CBDC software code to limit transactions or the scope of functionality for these unhosted wallets.

- **CBDCs will not replace conventional payment methods.** For the foreseeable future, an economy using CBDC will still keep other payment instruments. Banks will continue to accept deposits and provide traditional credit, wire transfers, debit cards, and other banking services. People could continue to use online payment companies that operate with traditional bank accounts instead of CBDC tokens. However, financial institutions and

various CBDC software wallet companies will likely partner to allow CBDC customers to exchange between traditional bank accounts and CBDC tokens.

- **CBDCs will interoperate with other financial instruments.** Retail merchants will accept CBDCs for online and in-person commerce. CBDC and financial institutions will offer easy avenues for their bank customers to move between CBDCs, deposits, physical cash, and other instruments or assets. For example, it might be possible for bank customers to withdraw their savings accounts as CBDC onto their digital wallets and to add funds to their stock portfolios through the same CBDC wallets.

- **Other cryptoassets are not going away.** Other independent cryptoassets such as Bitcoin, Ethereum, and various stablecoins based on public, permissionless blockchains will continue to exist alongside CBDCs. Their usage could decline as the public adopts CBDC, but it is also plausible that these decentralized tokens could gain adoption in specific use cases. AML regulatory challenges around the pseudonymity of cryptoassets will continue. Importantly, it should be assumed that some highly regulated cryptoasset exchanges will offer both CBDCs and independent, decentralized cryptoassets.

CBDC functionality will enable much innovation for perfectly legitimate purposes. For example, payment interface providers could potentially give users dozens or hundreds of wallets to organize their payments around certain categories or specifications. A user could hold specific wallets for food purchases, transportation costs, recreational spending, emergency repairs, and charitable giving and also set up wallets for transacting with individual family members or businesses. For example, the People's Bank of China has stated that a CBDC wallet could be set up for a license plate only to pay the driver's parking and toll fees.[37] So, with CBDCs, individuals could potentially create a wallet for any item they owned to conduct transactions with people or sensor-based machine applications. A car could have a wallet, but so could one's television, solar panel, or computer server. Customizations like these could help with personal budgeting and tracking spending, but they are not easily done with today's bank accounts.

Software applications built on if-then contracts between different wallet users will offer new and smarter types of transaction arrangements. For example, a buyer of a sailboat could easily set up a digital contract and an escrow wallet with the seller. This wallet could be programmed so that it releases funds to the seller only after certain conditions have been met, such as the boat passing

[37] CBNEditor, "China's Statutory Digital Currency Won't Undermine Mobile Payments: Central Bank's CBDC Chief," *China Banking News*, June 15, 2020, www.chinabankingnews.com/2020/06/15/chinas-statutory-digital-currency-wont-undermine-mobile-payments-central-banks-cbdc-chief/.

inspection and the title being found clear of any liens. In another scenario, a news publication could program its website to pay authors CBDC instantly from a portion of readers' CBDC spent to access individual articles. Micropayments would allow for a variety of such arrangements, especially for transactions involving "internet of things" devices.

Such functionality programmed into CBDC wallets by smart contracts will likely generate innovations that are not yet conceivable, just as many of today's mobile apps could not have been envisioned before the creation of smartphones.

MONEY LAUNDERING WILL EVOLVE TO ACCOMMODATE CBDC

The first level of CBDC management, where the central bank oversees the development of digital currency and disburses it to payment interface providers, is likely to face significant cybersecurity threats. State actors conducting cyber-enabled economic warfare might be the main perpetrators of threats at this level.[38] This cybersecurity risk should not be dismissed. It is an existential threat to the integrity of a CBDC system. Policymakers will need to address critical cybersecurity vulnerabilities sufficiently before deploying a CBDC fully. Analysis of CBDC cybersecurity risks deserves its own treatment outside of this paper.

For our discussion, we will assume that the CBDC's first tier is sufficiently secure from a cybersecurity perspective. Our focus on the second tier will consider end users' transactions with each other, through payment interface provider software. The payment interface provider–to–user layer will be public facing and in 24/7 retail use. Thus, it will be a wide target for illicit finance.

For financial regulators, the impact of a CBDC on illicit finance is likely to be both positive and negative. The good news is that a CBDC will likely hinder direct criminal use. Illicit actors in most cases will prefer cash over CBDC in funding illegal activities, because cash will remain anonymous, whereas CBDC will have a documented identity attached to each digital wallet and, thus, each transaction. Although law enforcement would not have direct, real-time access to this information, the data would offer a digital "paper trail" that authorities could potentially acquire. Therefore, operating with pure anonymity, as with cash, would be impossible for criminals using CBDC. Illicit

[38] "U.S. Government and Private Industry Must Prepare for Cyber-Enabled Economic Warfare Escalations," Foundation for Defense of Democracies, Feb. 5, 2019, www.fdd.org/wp-content/uploads/2019/02/memo-ceew-wargame.pdf; U.S. Department of Homeland Security, "Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar, 2019, www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf.

actors would need either to take on the risk of transacting in CBDC under their true identity or to go through the trouble to construct a fake identity, steal someone's identity credentials, or get a witting person to allow them to use their CBDC wallet.

The bad news is that, because CBDC would be widely accepted by merchants and have some novel technical features such as micropayments and programmability, criminals will still want to acquire it. Therefore, financial authorities should expect to encounter elaborate money laundering schemes by illicit actors trying to get dirty money into the CBDC system. The financial crime risk for CBDCs is less about users paying for illicit activity and more about criminals offloading illicit proceeds into CBDCs.

In particular, illicit actors will likely adapt to the rollout of a CBDC by developing more sophisticated money laundering schemes that trade cash and anonymous digital tokens for CBDC through layers of underground and ostensibly legitimate transactions. Law enforcement has long understood "layering" as a key component of the money laundering process, whatever the technology.[39] The layering is followed by "integrating" the seemingly clean funds back into the formal financial system.[40] When checks, credit cards, and online payments such as PayPal came into existence, they brought in new typologies of illicit activity, ranging from fraud and scams to identity theft and elaborate money laundering. CBDCs will likely follow a similar path.

Four factors will facilitate money laundering in CBDCs: money mules, complicit merchants, the ease of cross-border transactions, and the availability of noncompliant cryptoasset exchanges. Illicit actors are likely to use some or all of these elements to obfuscate the illicit money transactions occurring outside of CBDCs and bring dirty money into the CBDC ecosystem.

Money Mules

The FBI defines a money mule as "someone who transfers illegally acquired money on behalf of or at the direction of another."[41] Criminal organizations often feed "dirty" cash to someone who is ostensibly unconnected to their activity so that person can put the illicit funds into a bank account. Once the money is in the banking system, the mule can send funds to another account controlled by

[39] Financial Action Task Force, "Professional Money Laundering, July 2018, www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf.
[40] Financial Crimes Enforcement Network, "History of Anti-Money Laundering Laws," 2020, www.fincen.gov/history-anti-money-laundering-laws.
[41] Federal Bureau of Investigation, "Money Mule Awareness Booklet," Dec. 17, 2018, www.fbi.gov/file-repository/money-mule-awareness-booklet.pdf/view.

the criminal's network or purchase goods and services for the network. If CBDCs are available only through regulated platforms that use know-your-customer processes, then criminals will likely build a network of CBDC money mules whom they use to turn illicit physical cash into clean CBDC tokens.

CBDC money mule operations are likely to be more intricate than traditional ones because they would be able to exploit various tools derived from computer science. The programmable nature of CBDCs would allow payment interface providers to design wallets with more functionality than today's bank accounts. Money mules could use multiple wallets as fronts for criminal transfers, conduct hundreds or thousands of small CBDC transactions over time, and build a web of programmable transactions to obfuscate the origins of illicit money entering the CBDC system. This laundering technique is already familiar to cybercriminals, including nation-state actors. For example, in early 2020, the U.S. Department of Justice indicted two Chinese nationals for laundering more than $100 million worth of cryptoassets that North Korean regime operatives hacked from a cryptocurrency exchange.[42] Using simple computer programs, the launderers moved stolen tokens between various digital wallets through thousands of transactions to try to conceal the funds' origins.[43]

In a CBDC environment with smart-contract functionality, a single person could potentially manage hundreds of digital wallets and exploit various automated features (many of which probably have not been thought of yet). CBDC money mules would have more flexibility in the types of transactions they could generate and hide behind, compared to money mules using only bank account services.

Witting Merchants

A key subtype of money mules are witting merchants: retail merchants who agree to be fronts to move illicit funds through the CBDC ecosystem. Witting merchants are effective money mules because they have a high volume of legitimate business transactions to help conceal illicit proceeds.

---

[42] Yaya J. Fanusie, "Cryptocurrency Laundering Is a National Security Risk," *Lawfare*, March 31, 2020, www.lawfareblog.com/cryptocurrency-laundering-national-security-risk.
[43] U.S. District Court for the District of Colombia, *United States of America v. 113 Virtual Currency Accounts*, March 2, 2020, www.justice.gov/opa/press-release/file/1253491/download.

Witting merchants could facilitate a variation on trade-based money laundering, which involves falsifying invoices in order to transfer illicit value through import or export transactions.[44] Trade-based money laundering is commonly associated with cross-border business, but much of the methodology is applicable to domestic transactions. One way this could play out would be for an industrial supplies retailer to receive illicit physical cash from a criminal and then sell equipment to the criminal (or the criminal's money mule) for CBDC at an extremely low price, by falsifying either the quality or quantity of the equipment on the invoice. The criminal could then sell the equipment for CBDC at full price in a legitimate market so that he has an amount in CBDC close to what he initially gave the witting merchant in dirty cash.

However, CBDC laundering may be easier with merchants who offer services that are not delivered physically. A witting vendor who provides online or virtual services could have a whole set of clients who are really money mules, requiring no storefront, office location, or supply room. The mules could send the merchant CBDC for services that have never been performed. The merchant might spend the CBDC on a variety of digital services or might purchase physical goods, all on behalf of her criminal sponsor, but disguised as business or personal expenditures. This type of laundering occurs today but will likely increase as CBDCs widen the range of digital commerce in the economy. And as more "internet of things" devices connect to CBDC payment applications, an entire ecosystem of laundering is likely to arise.

Ease of Cross-Border Transactions

One of the biggest potential advantages of a CBDC is greater speed and efficiency in international transfers. Much CBDC research today focuses on applying the technology to cross-border transactions.[45] Criminal networks use a bevy of schemes to move money internationally through banks, money transfer services, and hawalas (traditional money transmitters, popular in Muslim-majority countries). But such international transactions are often riskier than domestic ones. They involve more than one jurisdiction and thus raise the possibility of discovery from multiple law enforcement bodies. And since cross-border transactions often go through a clearing process involving different currencies and different banking regulators, it may take longer for parties to confirm the success of a transfer.

---

[44] John Cassara, "Modernizing AML Laws to Combat Money Laundering and Terrorist Financing," Nov. 28, 2017, https://www.judiciary.senate.gov/imo/media/doc/Cassara%20Testimony.pdf.
[45] Raphael Auer et al., "Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies" (BIS Working Papers No. 880), Bank for International Settlements, 2020, www.bis.org/publ/work880.pdf.

A CBDC could eliminate this friction. A CBDC white paper by the U.S.-based blockchain technology firm R3 proposes "atomic payments" for cross-border transactions where the transfer happens risk free:[46] The international CBDC transaction in one currency is programmed to depend on a corresponding foreign exchange transaction in the other nation's CBDC system.[47] Assuming multiple nations have their own CBDCs, it would be much easier to conduct international transactions and to automate them using programmable digital wallets. This would expand the scope of international schemes and would require more technological sophistication to detect.

Noncompliant Cryptoasset Exchanges

As long as an online market exists where users can purchase pseudonymous cryptoassets, there will likely be some noncompliant exchanges where criminals go to launder funds. Illicit funds moving to noncompliant exchanges and onto wallets that interact with compliant exchanges are likely to end up getting traded eventually for CBDCs, if regulated cryptoasset exchanges also offer central bank digital currencies. Trading on darknet markets will also continue, not using CBDC, but via pseudonymous digital currencies. In fact, anonymity-enhancing tokens such as Monero are likely to proliferate in an underground, peer-to-peer cryptoasset ecosystem[48] as they become less welcome on regulated markets.[49] And some blockchain programmers are working to expand anonymity in the cryptoassets environment by trying to make the Bitcoin protocol more private[50] and building new anonymity-preserving blockchains.[51] Money launderers will continue to exploit pseudonymity and anonymity, moving illicit cryptoasset proceeds from ransomware, darknet activity, or human trafficking onto exchanges with lax or no AML and know-your-customer restrictions. From there, criminals can convert funds into fiat currencies and purchase CBDCs. The regulated and

---

[46] R3, "Central Bank Digital Currency: An Innovation in Payments," April 2020, www.r3.com/wp-content/uploads/2020/04/r3_CBDC_report.pdf.
[47] Bank of England, "Central Bank Digital Currency Opportunities, Challenges and Design."
[48] Yaya J. Fanusie, "Financial Authorities Confront Two Cryptocurrency Ecosystems," Council on Foreign Relations, October 11, 2018, cdn.cfr.org/sites/default/files/pdf/Discussion_Paper_Collection_Kahler_et_al_IFFs_OR_Fanusie.pdf.
[49] Daniel Palmer, "Another Crypto Exchange Is Dropping Privacy Coin Monero Over Compliance Risk," CoinDesk, Dec. 2, 2019, www.coindesk.com/another-crypto-exchange-is-dropping-privacy-coin-monero-over-compliance-risk.
[50] Alyssa Hertig, "Schnoor/Taproot Could Improve Bitcoin Privacy and Scaling," CoinDesk, April 7, 2020, www.coindesk.com/bitcoins-future-exactly-how-a-coming-upgrade-could-improve-privacy-and-scaling.
[51] Mike Orcutt, "A New Harry Potter–Themed Cryptocurrency Is Like a More Private Version of Bitcoin," *MIT Technology Review*, April 2, 2020, www.technologyreview.com/2019/01/31/137637/a-new-harry-potterthemed-cryptocurrency-is-like-a-more-private-version-of-bitcoin/.

unregulated ecosystems will continue to operate in parallel and mix where illicit actors are able to move between them.

Some recent cases show how illicit actors advance criminal schemes by exploiting jurisdictions with poorly regulated cryptoasset exchanges. In June 2020, members of a Romanian-based network pleaded guilty to an international cyber racketeering scheme. The members scammed victims in the United States out of Bitcoin, which they transferred to a co-conspirator who owned a Romanian cryptoasset exchange. The exchange owner then converted the tokens to fiat currency and placed them into bank accounts he controlled.[52]

Also in June 2020, Estonia's Financial Intelligence Unit revoked the licenses of more than 500 cryptoasset exchanges that had registered in the small nation. The Estonian authorities cited examples of embezzlement occurring through the exchanges, with licenses enabling criminals to "create credibility for some evil schemes."[53]

Laundering darknet market proceeds through unregulated exchanges is a long-standing cryptoasset laundering technique.[54] Even as more exchanges are now following AML regulations, many remain noncompliant and attract illicit customers. By early 2020, leaked documents[55] revealed that the FBI found darknet vendors sending bitcoins they received to a website called MorphToken to exchange them into the anonymity-preserving token Monero. MorphToken is a Panama-incorporated exchange[56] known for allowing anonymous trading.[57] As long as exchanges with no know-your-customer controls exist, illicit actors will be able to send illicitly derived cryptoassets to money mules and front companies to operate on the illicit actors' behalf.

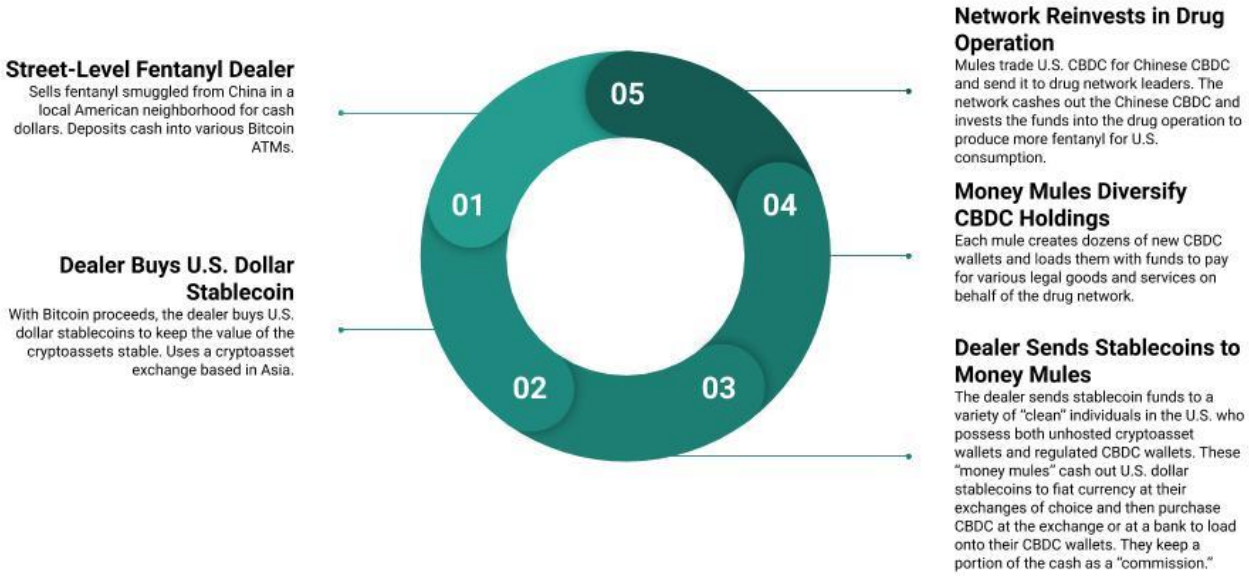
---

[52] U.S. Department of Justice, "Fifteen Defendants Plead Guilty to Racketeering Conspiracy in International Cyber Fraud Scheme" (press release), June 11, 2020, www.justice.gov/opa/pr/fifteen-defendants-plead-guilty-racketeering-conspiracy-international-cyber-fraud-scheme.
[53] Ott Ummelas, "EU Nation at Center of Dirty-Cash Storm Cracks Down on Crypto," Bloomberg, June 11, 2020, www.bloomberg.com/news/articles/2020-06-11/eu-nation-at-center-of-dirty-cash-storm-cracks-down-on-crypto.
[54] Yaya J. Fanusie and Tom Robinson, "Bitcoin Laundering: An Analysis of Illicit Flows Into Digital Currency Services," Foundation for Defense of Democracies, Jan. 12, 2018, www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf.
[55] Timothy Lloyd, "Blueleaks: How the FBI Tracks Bitcoin Laundering on the Dark Web," Decrypt, July 10, 2020, decrypt.co/34740/blueleaks-how-the-fbi-tracks-bitcoin-laundering-on-the-dark-web.
[56] MorphToken, 2020, www.morphtoken.com/terms/.
[57] J.P. Buntinx, "Top 3 ShapeShift Alternatives Without KYC Requirements," NullTX, Sept. 6, 2018, nulltx.com/top-3-shapeshift-alternatives-without-kyc-requirements/.

Illicit actors will likely exploit a variety of other features in the cryptoasset space in order to launder funds into CBDCs. They might use stablecoins,[58] which peg a specific asset or basket of assets to a digital token in order to mitigate price and exchange-rate volatility. Chinese traders in underground markets in Russia have used stablecoins and over-the-counter cryptoasset exchanges to circumvent capital controls and tax requirements.[59] In addition, criminals regularly use software tools such as cryptoasset mixers and tumblers to obfuscate illicit payments.[60]

HYPOTHETICAL ILLICIT FINANCE SCENARIOS INVOLVING CBDC

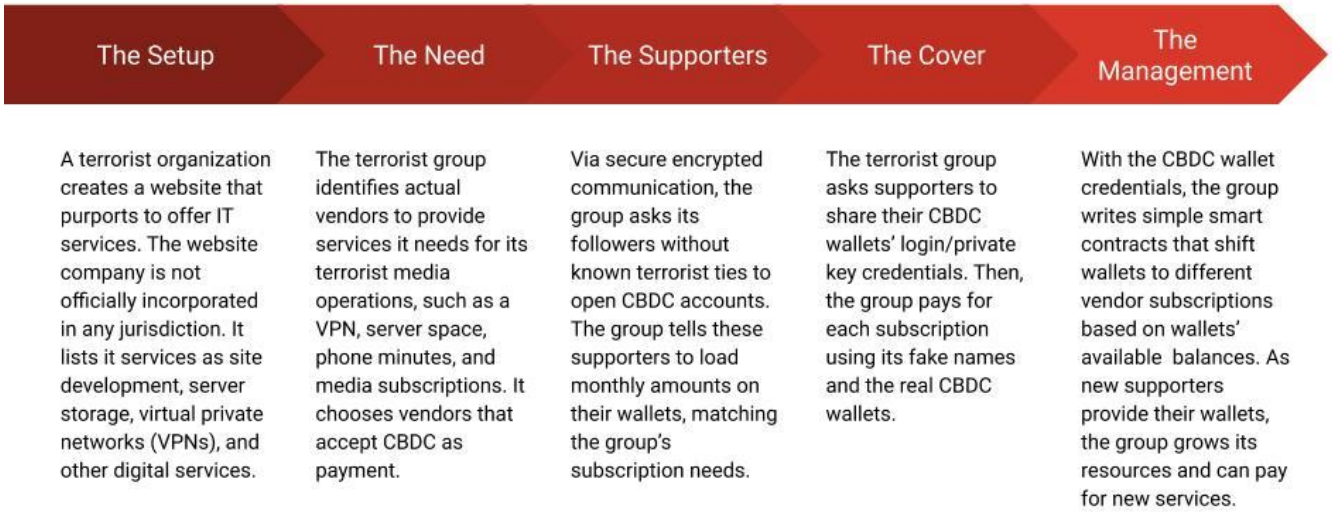
Financial authorities considering launching a CBDC must think carefully about how criminals will try to transfer their loot into the regulated CBDC ecosystem. The following hypothetical scenarios illustrate how illicit actors might infuse financial crime proceeds into CBDCs and how financial authorities could mitigate such activity on a tactical level.



[58] Financial Stability Board, "Addressing the Regulatory, Supervisory and Oversight Challenges Raised by 'Global Stablecoin' Arrangements," April 14, 2020, www.fsb.org/wp-content/uploads/P140420-1.pdf.
[59] Anna Baydakova, "Millions in Crypto Is Crossing the Russia-China Border Daily. There, Tether Is King," CoinDesk, July 30, 2019, www.coindesk.com/tether-usdt-russia-china-importers.
[60] U.S. Department of Justice, "Ohio Resident Charged With Operating Darknet-Based Bitcoin 'Mixer,' Which Laundered Over $300 Million" (press release), Feb. 13, 2020, www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million.

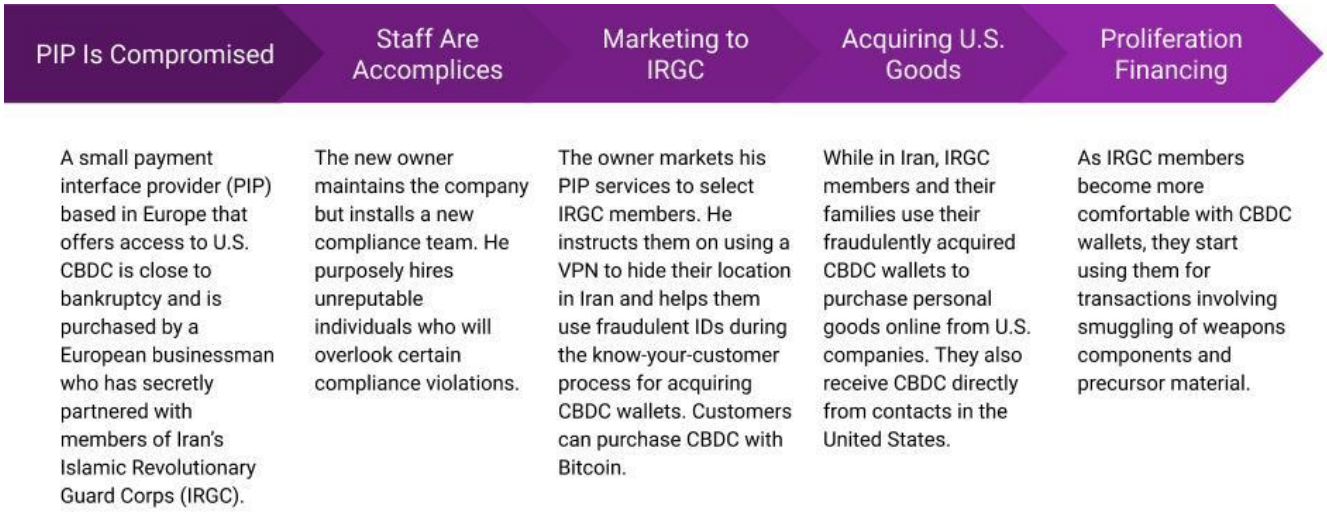
Scenario A: Chinese-produced fentanyl cash laundered with cryptoassets and CBDC. In this scenario, a China-based fentanyl distribution network turns its cash proceeds from street dealers in the United States into the cryptoasset Bitcoin. However, because of Bitcoin's high volatility and minimal merchant acceptance, the dealer then buys stablecoins to preserve the U.S. dollar value and sends them to money mules who also hold CBDC wallets. Operating in CBDCs allows the money mules to set up multiple wallets that could be used to pay for goods and services on the network's behalf. In cases where payment interface providers enforce transaction limits, the mules would conduct "structuring," where launderers break up large-volume payments into multiple smaller ones in order to transact under regulatory limits and avoid AML scrutiny. The money mules can trade U.S. CBDC for Chinese CBDC, which allows the network to cash out renminbi to reinvest into its ongoing production and smuggling operation.

Tactical Countermeasures: To counter this operation, financial authorities in the United States should ensure payment interface providers are using proper know-your-customer controls and conducting risk-based due diligence of customers onboarding to CBDC wallets. Also, payment interface providers should use transaction monitoring systems to flag suspicious activity. These are standard practices in AML compliance, but additional fine-tuning will be needed to determine how structuring and other laundering methods manifest using CBDC wallets and smart contracts. Compliance teams should consult the September 2020 report on "Virtual Assets Red Flag Indicators" by the Financial Action Task Force, the international standard-setting body for AML. The report provides insights about laundering methodologies that various countries have observed happening through digital assets. Also, financial intelligence units around the world must work to implement the Financial Action Task Force's broader regulatory guidance on virtual assets in order to lessen the number of virtual asset service providers that allow users to trade cryptoassets with insufficient AML and know-your-customer controls.



Scenario B: Terrorists funding digital services with CBDC wallets. In this scenario, a terrorist group creates a fake IT company as a cover for purchasing services to support its cyber and media operations and internal communications. Because the terrorist organizers cannot easily acquire CBDC wallets due to the payment interface providers' know-your-customer process, they ask supporters to share CBDC wallet credentials. Because most merchant transactions do not require AML obligations, the actual vendors do not verify identities of people simply purchasing their services. So, the terrorists purchase monthly IT and media services with their supporters' wallets. Given CBDC programmability, the terrorists are able to manage the payments through multiple wallets, shifting streams from one wallet to another as needed and adding new wallet streams as new supporters share their CBDC credentials.

Tactical Countermeasures: The payment interface providers would be the major line of defense against this scenario. If the terrorist supporters have no overt nefarious links, they might not raise flags during the know-your-customer process when acquiring their CBDC wallets. However, the payment interface providers should conduct transaction monitoring to flag possible suspicious activity such as wallets being accessed in an unexpected geographic location or other anomalous use or patterns. A complicating factor would be if the terrorist supporters use an unhosted CBDC wallet, which, although it has an identity attached, is not monitored as closely as hosted wallets. Specific rules and architecture around unhosted CBDC wallets would be critical for mitigating this threat. Also, law enforcement and intelligence officials should uncover the financial links to such terrorist groups by identifying and investigating vendors that the group is using for its media operations and communications.



Scenario C: A payment interface provider facilitates sanctions evasion. In this scenario, an unscrupulous businessman purchases a payment interface provider firm in order to facilitate purchases that violate U.S. sanctions against Iran. By ignoring sanctions compliance rules and procedures, the payment interface provider becomes an instrument for funding members of Iran's Islamic Revolutionary Guard Corps and supporting their proliferation and smuggling operations.

Tactical Countermeasures: Here, the regulatory oversight of the payment interface provider is key to prevent such illicit activity. As a firm that holds and exchanges U.S. CBDC, the hypothetical payment interface provider in this scenario would still be subject to U.S. jurisdiction and the regulations of the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN).[61] The firm would need to be examined regularly for AML compliance.[62] Examiners should be sure to evaluate the professional standing and certifications of the firm's owner and employees, especially after a change in ownership.

POLICY RECCOMMENDATIONS

Because central banks are mostly in the early stages of their digital currency exploration, now is the best time to address questions about the risks and consequences that would come from deploying a

[61] Financial Crimes Enforcement Network, "Fact Sheet on MSB Registration Rule," 2020, www.fincen.gov/fact-sheet-msb-registration-rule.

[62] Financial Crimes Enforcement Network, "FinCEN Announces Release of Manual to Aid Examiners of Money Services Businesses" (press release), Dec. 9, 2008, www.fincen.gov/news/news-releases/fincen-announces-release-manual-aid-examiners-money-services-businesses#:~:text=FinCEN%20relies%20on%20the%20IRS,regulations%20that%20apply%20to%20MSBs.

central bank digital currency. In addition to the critical issue of a CBDC's technical security, policymakers need to explore what framework would best guide this technology's design and implementation. Much of the framework will have to consider inevitable second- and third-order effects on financial crime and money laundering that would originate outside of CBDCs. The following are key ways for U.S. policymakers, the private sector, and the broader public to prepare for these developments and ensure that a CBDC not only will support monetary effectiveness and financial innovation but also will hinder financial crime and safeguard privacy and civil liberties:

- **Integrate CBDC risks into the National Illicit Finance Strategy.** When the U.S. Treasury Department released the National Strategy for Combatting Terrorist and Other Illicit Financing in February 2020,[63] it contained only a passing reference[64] to CBDCs. Treasury should stand up and steer an interagency working group to coordinate deeper analysis on illicit financing risks accompanying CBDC deployments, whether by U.S. or foreign central banks. The working group should include personnel from the departments of Justice and Homeland Security, and members of the intelligence community. It should devote significant attention to the novel technical features of CBDCs and facilitate "war-gaming" simulations for how smart contracts could be exploited for money laundering purposes. The group should track the progress of CBDC pilots around the globe[65] and incorporate an analysis of CBDC risks into the broader U.S. national security strategy.

- **Establish a public-private partnership on CBDCs and privacy.** To address the privacy concerns that would arise from a CBDC system that records every user transaction, the United States needs more than just policy discussion. It requires a broader societal dialogue around financial privacy, constitutional protections, and American values. The U.S. Federal Reserve should coordinate a working group of public- and private-sector stakeholders to propose a CBDC privacy framework for the United States. This group should include members of the banking industry, financial technology specialists and computer science developers, privacy legal experts, and financial regulators. Although the group would not have any formal government oversight function, it should seek inspiration from the U.S. Privacy and Civil Liberties Oversight Board and its oversight reports.[66] The working group

[63] U.S. Department of the Treasury, "Treasury Announces 2020 National Illicit Finance Strategy" (press release), Feb. 6, 2020, www.home.treasury.gov/news/press-releases/sm902.
[64] U.S. Department of the Treasury, "National Strategy for Combating Terrorist and Other Illicit Financing," 2020, home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf.
[65] *CBDC Tracker - Central Bank Digital Currencies*.
[66] Privacy and Civil Liberties Oversight Board, "Oversight Reports," 2020, www.pclob.gov/Oversight.

should facilitate robust and balanced discussion of the privacy risks arising from both government and private-sector access to personal information in CBDC big data. The framework should consider the potential illicit financing risks accompanying CBDC deployment and outline ways to design CBDC anti-money laundering and know-your-customer requirements that will respect civil protections against unreasonable search and seizure. This working group should assess the viability of unhosted wallets in the CBDC system. It should also consider how much additional responsibility, if any, merchants should have for AML compliance if they accept CBDC for purchases. The U.S. government and the private sector should use such a framework in proposing global CBDC standards in consultation with international bodies such as the Financial Action Task Force, the Egmont Group, the Bank for International Settlements, the International Monetary Fund, and the Financial Stability Board.

- **Set more rigorous standards for CBDC payment interface providers.** The primary entities obligated to guard against layering and integrating illicit funds into CBDCs will be payment interface providers. Because CBDCs will be programmable, with a wider range of transactional capabilities than conventional financial accounts, regulators should consider raising the bar for money service businesses seeking licenses as CBDC payment interface providers. The ability for anyone with an internet connection to acquire and trade independent cryptoassets allows for a low barrier to entry that has contributed to the virtual asset sector's lag in AML compliance.[67] Regulated cryptoasset exchanges seeking to add a CBDC to their available digital assets should have to seek additional approval from FinCEN to do so. FinCEN should evaluate such exchanges and other money service businesses according to a risk-based due diligence standard similar to the Wolfsberg Correspondent Banking Due Diligence Questionnaire.[68] Evaluators should place particular attention on the ultimate beneficial ownership of payment interface providers, their business history, and their source of funds.

The prospect of a central bank digital currency offers much potential for financial innovation, efficiency, and inclusion. If or when a CBDC is deployed in a major economy such as the United States, there will be unintended consequences. Policymakers and society in general need to anticipate the dangers as much as possible. The economy's further digitization will lead to a new

[67] "Q3 2019 Cryptocurrency Anti-Money Laundering Report," CipherTrace, Feb. 10, 2020, ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/.
[68] The Wolfsberg Group, "Wolfsberg Group Questionnaires," Oct. 5, 2020, www.wolfsberg-principles.com/wolfsbergcb.

realm of commerce. A new realm of criminal exploitation will likely arise as well. But with sufficient effort, it can be countered.

The Digital Social Contract paper series is supported by funding from Facebook, which played no role in the selection of the specific topics or authors and which played no editorial role in the individual papers.